The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
10/12/2012

SUBJECT:
Multiple Vulnerabilities have been identified in Mozilla Products

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey applications. Mozilla Firefox is a web browser used to access theInternet. Mozilla Thunderbird is an e-mail client. Mozilla SeaMonkey is a cross platform Internet suite of tools ranging from a web browser to an e-mail client. Successful exploitation of these vulnerabilities could result in arbitrary code execution. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
- Firefox versions prior to 16.0.1
- Firefox Extended Support Release (ESR) versions prior to 10.0.9
- Thunderbird versions prior to 16.0.1
- Thunderbird Extended Support Release (ESR) versions prior to 10.0.9
- SeaMonkey versions prior to 2.13.1

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey. The details of these vulnerabilities are as follows:

- **Miscellaneous memory safety hazards (MFSA 2012-88)**
  Mozilla developers identified and fixed two top crashing bugs in the browser engine used in Firefox and other Mozilla-based products. These bugs showed evidence of memory corruption under certain circumstances, and we presume that with enough effort at least some of these could be exploited to run arbitrary code. The first of these bugs, a FreeType issue, is a mobile only issue which happens on custom kernels like Cyanogenmod, not on standard Android installations. The second bug is a web sockets crash affecting Firefox 16 but not Firefox ESR.

- **defaultValue security checks not applied (MFSA 2012-89)**
  Mozilla security researcher moz_bug_r_a4 reported a regression where security wrappers are unwrapped without doing a security check in defaultValue(). This can allow for improper access to the Location object. In versions 15 and earlier of affected products, there was also the potential for arbitrary code execution.

Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Upgrade vulnerable Mozilla products immediately after appropriate testing.
- Remind users not to visit untrusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Mozilla:

http://www.mozilla.org/security/announce/2012/mfsa2012-88.html
http://www.mozilla.org/security/announce/2012/mfsa2012-89.html

SecurityFocus:

http://www.securityfocus.com/bid/55889

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4190
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4191
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4192
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4193